

PCTWELTORGANISATION FÜR GEISTIGES EIGENTUM
Internationales BüroINTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE
INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

(5) Internationale Patentklassifikation ⁶ : H04L 9/32	A1	(11) Internationale Veröffentlichungsnummer: WO 99/48241 (43) Internationales Veröffentlichungsdatum: 23. September 1999 (23.09.99)
(21) Internationales Aktenzeichen: PCT/DE99/00415 (22) Internationales Anmeldedatum: 16. Februar 1999 (16.02.99) (30) Prioritätsdaten: 198 11 318.8 16. März 1998 (16.03.98) DE (71) Anmelder (für alle Bestimmungsstaaten ausser US): SIEMENS AKTIENGESELLSCHAFT [DE/DE]; Wittelsbacherplatz 2, D-80333 München (DE). (72) Erfinder; und (75) Erfinder/Anmelder (nur für US): ENTERROTTACHER, An- ton [DE/DE]; Gassnerstrasse 9, D-80639 München (DE). JAHNEN, Georg [DE/DE]; Raiffeisenstrasse 56, D-85716 Unterschleissheim (DE). (74) Gemeinsamer Vertreter: SIEMENS AKTIENGE- SELLSCHAFT; Postfach 22 16 34, D-80506 München (DE).		(81) Bestimmungsstaaten: US, europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE). Veröffentlicht <i>Mit internationalem Recherchenbericht. Vor Ablauf der für Änderungen der Ansprüche zugelassenen Frist; Veröffentlichung wird wiederholt falls Änderungen eintreffen.</i>
(54) Title: AUTHENTICATION OF KEY DEVICES (54) Bezeichnung: AUTHENTIFIZIERUNG VON SCHLÜSSELGERÄTEN (57) Abstract The invention relates to a method for authenticating key devices, using an asymmetrical coding scheme. According to said method, a certificate (Z) which is specific of the device is allocated to the key device. A group-specific signature code (pAD) and a group-specific signature (S(Z)) of the certificate (Z) are allocated to each key device, a group being composed of a limited number of key devices. (57) Zusammenfassung Die Erfindung betrifft ein Verfahren zur Authentifizierung von Schlüsselgeräten unter Verwendung eines asymmetrischen Verschlüsselungsverfahrens, bei dem dem Schlüsselgerät ein geräteindividuelles Zertifikat (Z) zugeordnet wird. Erfindungsgemäss ist jedem Schlüsselgerät ein gruppenspezifischer Signaturschlüssel (pAD) und eine gruppenspezifische Signatur (S(Z)) des Zertifikats (Z) zugeordnet, wobei eine Gruppe aus einer zahlenmässig begrenzten Anzahl von Schlüsselgeräten besteht.		

LEDIGLICH ZUR INFORMATION

Codes zur Identifizierung von PCT-Vertragsstaaten auf den Kopfbögen der Schriften, die internationale Anmeldungen gemäss dem PCT veröffentlichen.

AL	Albanien	ES	Spanien	LS	Lesotho	SI	Slowenien
AM	Armenien	FI	Finnland	LT	Litauen	SK	Slowakei
AT	Österreich	FR	Frankreich	LU	Luxemburg	SN	Senegal
AU	Australien	GA	Gabun	LV	Lettland	SZ	Swasiland
AZ	Aserbaidshan	GB	Vereinigtes Königreich	MC	Monaco	TD	Tschad
BA	Bosnien-Herzegowina	GE	Georgien	MD	Republik Moldau	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagaskar	TJ	Tadschikistan
BE	Belgien	GN	Guinea	MK	Die ehemalige jugoslawische Republik Mazedonien	TM	Turkmenistan
BF	Burkina Faso	GR	Griechenland	ML	Mali	TR	Türkei
BG	Bulgarien	HU	Ungarn	MN	Mongolei	TT	Trinidad und Tobago
BJ	Benin	IE	Irland	MR	Mauretanien	UA	Ukraine
BR	Brasilien	IL	Israel	MW	Malawi	UG	Uganda
BY	Belarus	IS	Island	MX	Mexiko	US	Vereinigte Staaten von Amerika
CA	Kanada	IT	Italien	NE	Niger	UZ	Usbekistan
CF	Zentralafrikanische Republik	JP	Japan	NL	Niederlande	VN	Vietnam
CG	Kongo	KE	Kenia	NO	Norwegen	YU	Jugoslawien
CH	Schweiz	KG	Kirgisistan	NZ	Neuseeland	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Demokratische Volksrepublik Korea	PL	Polen		
CM	Kamerun	KR	Republik Korea	PT	Portugal		
CN	China	KZ	Kasachstan	RO	Rumänien		
CU	Kuba	LC	St. Lucia	RU	Russische Föderation		
CZ	Tschechische Republik	LI	Liechtenstein	SD	Sudan		
DE	Deutschland	LK	Sri Lanka	SE	Schweden		
DK	Dänemark	LR	Liberia	SG	Singapur		
EE	Estland						

Beschreibung

Authentifizierung von Schlüsselgeräten

- 5 Die Erfindung betrifft ein Verfahren gemäß dem Oberbegriff des Patentanspruchs 1.

Ein solches Verfahren ist im Prinzip in dem Buch von W. Fumy und H.P. Rieß: Kryptographie, Entwurf und Analyse symmetrischer Kryptosysteme R. Oldenbourg Verlag, München Wien, 1988, ISBN 3-486-20868-3, beschrieben.

Bei verschlüsselter Übertragung von Sprache oder allgemeiner von Daten müssen beide Kommunikationspartner über ein gemeinsames Geheimnis verfügen, das Schlüsselwort. Dieses Schlüsselwort ist einem potentiellen Mithörer oder Gegner unbekannt. Eine Möglichkeit hierfür ist ein asymmetrisches Verschlüsselungsverfahren, bei dem Zufallszahlen zwischen den Kommunikationspartnern ausgetauscht und daraus gemeinsame Schlüsselworte gebildet werden.

Bei diesem Verfahren kann nicht festgestellt werden, ob die verschlüsselte Verbindung zu dem gewünschten Kommunikationspartner oder zu einem Gegner aufgebaut wird.

Kryptographische Verfahren können nicht nur zu Geheimhaltung, sondern auch zur Authentifizierung von Nachrichten eingesetzt werden. Die Verschlüsselung einer Nachricht unter Verwendung eines Schlüsselwortes beinhaltet im Prinzip auch deren Authentizität, da ein Gegner ohne Kenntnis des Schlüsselwortes den Klartext der Nachricht nicht erzeugen kann.

Bei einem asymmetrischen Kryptosystem wird für die Verschlüsselung einer Nachricht ein anderes Schlüsselwort verwendet, als für die Entschlüsselung. Ein solches System mit einem öffentlichen und einem privaten Schlüssel wird auch als Public Key System bezeichnet. Das bekannteste Beispiel für das Pu-

blic Key System ist das sogenannte RSA-Verfahren, dessen Grundzüge ebenfalls in der eingangs genannten Literaturstelle beschrieben sind.

- 5 Auf den ersten Blick wird das System der Schlüsselverteilung bei der Verwendung asymmetrischer Kryptosysteme weitgehend gelöst, da die öffentlichen Schlüssel problemlos über unsichere Datenkanäle ausgetauscht werden können. Dies ist aber nur richtig, solange man das Abhören als die einzige Gefähr-
- 10 dung einer Kommunikationsverbindung betrachtet. Neben passiven Abhörversuchen muss man in den meisten Fällen aber auch mit der Möglichkeit aktiver Angriffe rechnen. Hierbei schaltet sich ein aktiver Gegner in die Datenverbindung zwischen zwei Teilnehmer ein. Ein solcher Angriff kann nur bei Verwen-
- 15 dung von Authentifizierungsmaßnahmen erkannt werden.

Der Erfindung liegt die Aufgabe zugrunde, ein Verfahren anzugeben, durch das die an einem Datenaustausch beteiligten Schlüsselgeräte authentifiziert werden können.

20

Diese Aufgabe wird erfindungsgemäß durch die im Patentanspruch 1 angegebenen Merkmale gelöst.

- Im Folgenden wird die Erfindung anhand eines Ausführungsbeispiels beschrieben. Bei der Beschreibung werden folgende Abkürzungen verwendet:
- 25

E	Verschlüsselung
D	Entschlüsselung
30 A, B, X	Teilnehmer
AD	Administrator
p	öffentlicher Schlüssel
s	geheimer Schlüssel
pAD	Signaturschlüssel, entspricht dem öffentlichen
35	Schlüssel p des Administrators AD

3

- Z Zertifikat, entspricht dem öffentlichen Schlüssel
p, dem Namen und weiteren Angaben eines Teilnehmers
X
- S Signatur
- 5 S(Z) Signatur des Zertifikates Z

Die Erfindung geht von einem Kryptoverfahren aus, bei dem alle Verschlüsselungsgeräte mit einem gemeinsamen Public Key Schlüssel ausgestattet sind. Dieser öffentliche Schlüssel pAD wird von einer vertrauenswürdigen Instanz, einem sogenannten Administrator AD vergeben. Hierdurch kann prinzipiell jedes Gerät mit jedem kommunizieren, wobei die teilnehmenden Geräte authentifiziert sind.

15 In an sich bekannter Weise ist jedem Schlüsselgerät individuell ein Zertifikat Z zugeordnet, praktisch eine Art Name für dieses Gerät. Daneben enthält das Zertifikat Z, bei der Verwendung des Public-Key-Systems, den öffentlichen Schlüssel pX des Teilnehmers oder Benutzers X.

20 Erfindungsgemäß werden Benutzergruppen gebildet, deren Geräte mit einem gemeinsamen, gruppenspezifischen Signaturschlüssel pAD ausgestattet werden. Dieser Signaturschlüssel pAD ist der öffentliche Schlüssel pAD des Administrators AD. Er kann direkt im Gerät, oder er kann in Form anderer Speichermedien, beispielsweise auf Chipkarte, gespeichert sein. Eine solche Benutzergruppe weist eine beschränkte Anzahl von Teilnehmern auf. Hierdurch ist die Verbreitung des Signaturschlüssels pAD eingeschränkt.

30 In an sich bekannter Weise kann beim Administrator AD zu einem Zertifikat Z(X) eines Benutzers X eine Signatur S(Z(X)) erzeugt werden. Dabei wird das Zertifikat Z(X) mit dem geheimen Schlüssels sAD des Administrators AD verschlüsselt.

35

$$S(Z(X)) = E(Z(X), sAD)$$

Diese Signatur $S(Z(X))$ wird ebenfalls im Schlüsselgerät des Benutzers X fest oder mobil gespeichert.

5 Der geheime und der öffentliche Schlüssel s_{AD} , s_X und p_{AD} , p_X des Administrators AD beziehungsweise der Teilnehmer X sind Teil des Public Key Systems, das beispielsweise durch die RSA-Algorithmen realisiert ist.

10 Der gruppenspezifische Signaturschlüssels p_{AD} und die teilnehmerspezifische beziehungsweise gerätespezifische Signatur $S(Z(X))$ werden beispielsweise bei einer Ausgestaltung der Erfindung bei einer Erstinitialisierung auf das Schlüsselgerät geladen. Daneben ist im Schlüsselgerät das zugehörige Zertifikat $Z(X)$ gespeichert. Diese Daten können auch an den ent-
15 sprechenden Teilnehmer auf einer Chipkarte ausgehändigt werden. Für diese Vorgänge ist ein persönlicher Kontakt mit dem Administrator AD oder zumindest ein sicherer Übertragungskanal zu ihm notwendig.

20 Zur gesicherten Kommunikation wird eine Verbindung zwischen den Teilnehmern A und B, das heißt zwischen den zugehörigen Schlüsselgeräten aufgebaut. Der Teilnehmer A überträgt zum Teilnehmer B das Zertifikat $Z(A)$ und die Signatur $S(Z(A))$. Der Teilnehmer B kann unter Verwendung des Signaturschlüssels
25 p_{AD} , das heißt des öffentlichen Schlüssels p des Administrators AD, die Echtheit des Zertifikates $Z(A)$, das heißt die Echtheit des Teilnehmers A verifizieren:

$$D(S(Z(A)), p_{AD}) = D(E(Z(A), s_{AD}), p_{AD}) = Z(A)$$

30

Analog überprüft der Teilnehmer A den Teilnehmer B.

Ein potentieller Angreifer ist gruppenfremd, besitzt keine vom Administrator AD ausgestellte Signatur S , und kann daher
35 zu keinem Teilnehmer dieser Gruppe eine Verbindung aufbauen, .

Bei einem Diebstahl werden die entsprechenden Geräte von der Benutzergruppe ausgeschlossen, so daß sie für einen Angreifer unbrauchbar werden. Hierzu ist bei einer möglichen Ausgestaltung der Erfindung im Schlüsselgerät eine Liste der zugelassenen Teilnehmer beziehungsweise der Schlüsselgeräte gespeichert. Es können die Identitäten der möglichen Schlüsselgeräte hinterlegt sein, und in den Verbindungsaufbau ist eine entsprechende Sicherheitsabfrage integriert.

Patentansprüche

1. Verfahren zur Authentifizierung von Schlüsselgeräten unter Verwendung eines asymmetrischen Verschlüsselungsverfahrens,
5 bei dem dem Schlüsselgerät ein geräteindividuelles Zertifikat (Z) zugeordnet wird,
dadurch gekennzeichnet,
dass jedem Schlüsselgerät ein gruppenspezifischer Signaturschlüssel (pAD) und eine gruppenspezifische Signatur (S(Z))
10 des Zertifikats (Z) zugeordnet wird, wobei eine Gruppe aus einer zahlenmäßig begrenzten Anzahl von Schlüsselgeräten besteht.
2. Verfahren nach Anspruch 1,
15 dadurch gekennzeichnet,
dass der Signaturschlüssel (pAD) und die Signatur (S(Z)) bei einer einmaligen Erstinitialisierung vergeben wird.
3. Verfahren nach Anspruch 1 oder 2,
20 dadurch gekennzeichnet,
dass die Gruppenzugehörigkeit durch Vergleich mit einer Liste ermittelt wird.

INTERNATIONAL SEARCH REPORT

International Application No

PCT/DE 99/00415

A. CLASSIFICATION OF SUBJECT MATTER

IPC 6 H04L9/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 6 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 97 48208 A (ERICSSON TELEFON AB L M) 18 December 1997 (1997-12-18) abstract page 5, line 22 - line 29 page 6, line 7 - page 7, line 6 figures 1,2,4	1,2
A	FR 2 709 903 A (THOMSON CSF) 17 March 1995 (1995-03-17) abstract page 4, line 10 - line 34 page 6, line 1 - line 8 claim 1 figures 1-3	1,3
	--- -/--	

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search

21 July 1999

Date of mailing of the international search report

29/07/1999

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Gautier, L

INTERNATIONAL SEARCH REPORT

Inter. l. Application No

PCT/DE 99/00415

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	<p>WO 95 14283 A (HUGHES AIRCRAFT CO)</p> <p>26 May 1995 (1995-05-26)</p> <p>page 1-4</p> <p>figure 1</p> <p>-----</p>	1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/DE 99/00415

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9748208 A	18-12-1997	US 5729537 A AU 3199697 A CA 2258036 A EP 0904643 A	17-03-1998 07-01-1998 18-12-1997 31-03-1999
FR 2709903 A	17-03-1995	NONE	
WO 9514283 A	26-05-1995	AU 669828 B AU 8095794 A CA 2149744 A,C EP 0682832 A JP 2723365 B JP 8512445 T NO 952584 A US 5825300 A	20-06-1996 06-06-1995 09-05-1995 22-11-1995 09-03-1998 24-12-1996 27-06-1995 20-10-1998

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen

PCT/DE 99/00415

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 6 H04L9/32

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierte Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 6 H04L

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie ^a	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	WO 97 48208 A (ERICSSON TELEFON AB L M) 18. Dezember 1997 (1997-12-18) Zusammenfassung Seite 5, Zeile 22 - Zeile 29 Seite 6, Zeile 7 - Seite 7, Zeile 6 Abbildungen 1,2,4	1,2
A	FR 2 709 903 A (THOMSON CSF) 17. März 1995 (1995-03-17) Zusammenfassung Seite 4, Zeile 10 - Zeile 34 Seite 6, Zeile 1 - Zeile 8 Anspruch 1 Abbildungen 1-3	1,3
	--- -/--	

☒ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

☒ Siehe Anhang Patentfamilie

^a Besondere Kategorien von angegebenen Veröffentlichungen:

"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist

"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist

"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)

"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht

"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist

"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderscher Tätigkeit beruhend betrachtet werden

"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderscher Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist

"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche

21. Juli 1999

Absenddatum des internationalen Recherchenberichts

29/07/1999

Name und Postanschrift der internationalen Recherchenbehörde
Europäisches Patentamt, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Bevollmächtigter Bediensteter

Gautier, L

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen

PCT/DE 99/00415

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	<p>WO 95 14283 A (HUGHES AIRCRAFT CO)</p> <p>26. Mai 1995 (1995-05-26)</p> <p>Seite 1-4</p> <p>Abbildung 1</p> <p>-----</p>	1

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen

PCT/DE 99/00415

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
WO 9748208 A	18-12-1997	US 5729537 A	17-03-1998
		AU 3199697 A	07-01-1998
		CA 2258036 A	18-12-1997
		EP 0904643 A	31-03-1999
FR 2709903 A	17-03-1995	KEINE	
WO 9514283 A	26-05-1995	AU 669828 B	20-06-1996
		AU 8095794 A	06-06-1995
		CA 2149744 A,C	09-05-1995
		EP 0682832 A	22-11-1995
		JP 2723365 B	09-03-1998
		JP 8512445 T	24-12-1996
		NO 952584 A	27-06-1995
		US 5825300 A	20-10-1998

This Page Blank (uspto)